Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ТЕСТИРОВАНИЕ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Ю.С. ХАРИН,

НИИ прикладных проблем математики и информатики БГУ

Введение

Случайные и псевдослучайные последовательности, а также их генераторы являются неотъемлемыми элементами современных систем криптографической защиты информации для решения следующих основных задач [1-3]: генерация гаммы в поточных криптосистемах; генерация сеансовых и других ключей в криптосистемах; генерация «случайных значений» параметров для многих систем ЭЦП; формирование «случайных запросов» при реализации большинства существующих криптографических протоколов выработки общего секретного ключа и аутентификации.

Генерация случайной последовательности с произвольным законом распределения вероятностей сводится к генерации равномерно распределенной случайной последовательности (РРСП). РРСП – это последовательность дискретных случайных величин $x_1, x_2, \ldots \in A = \{0,1,\ldots,N-1\}$ из конечного алфавита A мощности $2 \le N < +\infty$, обладающая двумя свойствами (гипотеза H_0):

C_1) для любого числа $n \in \mathrm{N}$ и произвольных индексов $1 < t_1 < \ldots < t_n$ случайные биты $x_{t_1}, \ldots, x_{t_n}$ независимы в совокупности;

C_2) для любого $t \in \mathrm{N}$ случайная величина x_t имеет равномерное на A распределение вероятностей: $\mathrm{P}\{x_t = i\} = N^{-1}$, $i \in A$.

В настоящее время известно более сотни методов и алгоритмов генерации последовательностей, по своим свойствам приближающихся к РРСП. Еще больше разработано методов статистического тестирования последовательностей.

В статье представлены аналитический обзор современного состояния в области тестирования криптографических генераторов случайных и псевдослучайных последовательностей, а также перспективные методы тестирования на основе моделей стохастических зависимостей высокого порядка.

1. Аналитический обзор методов тестирования

Генератор РРСП – это устройство, позволяющее по запросу получить реализацию равномерно распределенной случайной последовательности $x_1, x_2, \ldots, x_n \in A$ заданной длины n. В настоящее время в криптосистемах используются физические генераторы случайных последовательностей и программные генераторы псевдослучайных последовательностей (ПСП).

Физические генераторы используют случайность, **измеряемую** в некоторых физических процессах: квантовые процессы, шумовые колебания в резисторах и полупроводниковых диодах, частотные колебания осциллятора и другие. Основные требования, предъявляемые к физическим генераторам: «статистическая безопасность», стабильность вероятностных свойств генерируемой последовательности; эффективная аппаратная реализация. Главным достоинством физических генераторов является то, что выходная последовательность «лучше» удовлетворяет свойству C_1. Однако физические генераторы имеют также ряд недостатков: в выходной последовательности могут воз-

никать зависимости и отклонения от равномерного распределения вероятностей, вызванные наличием погрешностей измерений; практическая невозможность повторного воспроизведения выходной последовательности, что не позволяет использовать физические генераторы для синхронной генерации ключевой последовательности при поточном шифровании; проверка соответствия образца заявленному описанию иногда невозможна без разрушения генератора.

Генератор ПСП – это компьютерная программа или программно-аппаратное устройство для имитации реализации РРСП. Имитируемая последовательность $\{x_t\}$ называется псевдослучайной, т. к. она **вычисляется** на компьютере по известному детерминированному (обычно рекуррентному) соотношению, и в тоже время ее статистические свойства «близки» (по определенным статистическим критериям) к свойствам РРСП. К генераторам ПСП, используемым в криптосистемах, предъявляются следующие требования: «большой период»; «статистическая безопасность»; криптографическая стойкость; эффективная программная и аппаратная реализация.

Важнейшим требованием, предъявляемым как к физическим генераторам случайных последовательностей, так и к генераторам ПСП является требование «статистической безопасности». Оно заключается в том, что при используемой длине n генерируемых реализаций их невозможно отличить от реализаций РРСП на заданном уровне значимости $\varepsilon \in (0,1)$. Для проверки этого требования используются статистические тесты (критерии). Статистический тест – это решающее правило, позволяющее по наблюдаемой реализации $x_1,\ldots,x_n \in A$ длины n (или конечной выборке таких реализаций) с заданным уровнем значимости осуществить проверку гипотезы $H_0 = \{\{x_t\}$ есть РРСП$\}$ против некоторой альтернативы $H_1 = \bar{H}_0 = \{$нарушены свойства C_1, $C_2\}$. Существуют различные типы частных альтернатив H_1, каждый из которых порождает свой собственный статистический тест. Поэтому на практике при проверке требования «статистической безопасности» используют «батареи статистических тестов» [4-8]. Рассмотрим наиболее известные батареи тестов.

Исторически первой батарей тестов считается батарея статистических тестов, предложенная Д. Кнутом [4] и включающая в себя следующие тесты: частотный тест, тест серий; тест интервалов; покер-тест; тест собирателя купонов; тест перестановок; тест на монотонность; тест подпоследовательностей; тест «наибольшее из t». Большинство этих тестов являются частными случаями универсального алгоритма тестирования [3].

Батареей тестов, предъявляющей «более жесткие требования», чем батарея тестов Д. Кнута, является «DIEHARD»-батарея [5], которая предложена Дж. Марсальи в 1985 г. и содержит 16 тестов, приведенных в [3].

Третья батарея тестов предложена NIST [6] и включает следующие тесты: частотный тест; частотный тест внутри блока; тест серий; тест, основанный на рангах двоичных матриц; спектральный тест; универсальный статистический тест Маурера; тест, основанный на алгоритме сжатия Лемпеля – Зива; тест, основанный на линейной сложности; тест на основе аппроксимации энтропии и другие.

Батарея тестов CRYPT-X разработана австралийским Институтом Безопасности Информации [7] и включает 13 разделов.

Еще одна батарея тестов, используемая в конкурсе NESSIE [8], включает следующие тесты: фильтрующий тест; корреляционный тест; тест Неймана – Пирсона; тест серий; тест на основе линейной аппроксимации; частотный тест; тест на основе парадокса дней рождений; универсальный статистический тест Маурера; покер-тест;

тест, основанный на алгоритме сжатия Лемпеля – Зива; тест, основанный на нелинейной сложности; спектральный тест и другие.

Проведенный в [3] обзор существующих статистических тестов показывает:

1) многие из существующих тестов не ориентированы на проверку главного свойства C_1, а лишь частных случаев свойств C_1, C_2, т.е. частных случаев H_1;

2) многие из известных тестов построены «эвристически» и не фиксируют семейство альтернатив H_1;

3) многие тесты не имеют оценок мощности;

4) при включении нескольких тестов в батарею не удается оптимизировать «составной» тест.

В связи с этим актуальны задачи разработки адекватных вероятностных моделей для описания отклонений H_1 от модели РРСП, построения статистических тестов для обнаружения и оценивания таких отклонений, порожденных наличием стохастических зависимостей высокого порядка в выходной последовательности $\{x_t\}$.

2. Методы тестирования s-мерной равномерности на основе энтропийных характеристик

Определим вложенное в H_1 семейство «альтернатив s-мерной неравномерности»: $H_{1(s)} = \{\{x_1, x_2, \ldots\} = \{X_1, X_2, \ldots\}\} \subset H_1$, где $X_1, X_2, \ldots \in A^s$ – независимые одинаково распределенные s-фрагменты (слова) над алфавитом A с некоторым s-мерным дискретным распределением вероятностей $\mathrm{P}_{i_1,\ldots,i_s} = \mathrm{P}\{x_1 = i_1, \ldots, x_s = i_s\}$, $i_1, \ldots, i_s \in A$, отличным от равномерного:

$$\Delta_s = \sum_{i_1,\ldots,i_s \in A} \left| \mathrm{P}_{i_1,\ldots,i_s} - N^{-s} \right| > 0, \quad \sum_{i_1,\ldots,i_s \in A} \mathrm{P}_{i_1,\ldots,i_s} \equiv 1.$$

При $s \to \infty$ семейство этих альтернатив имеет в пределе альтернативу $H_1 = \bar{H}_0$ общего вида. Чем меньше Δ_s, тем ближе альтернатива $H_{1(s)}$ к нулевой гипотезе H_0.

Обозначим: $\{x_1, x_2, \ldots, x_T\} = \{X_1, X_2, \ldots, X_M\}$ – наблюдаемая реализация выходной последовательности длиной $T = M \cdot s$, разбитая на M непересекающихся фрагментов длины s, $\mathrm{I}\{B\}$ – индикатор события B,

$$\hat{\mathrm{P}}_{i_1,\ldots,i_s} = \frac{1}{M} \sum_{m=1}^{M} \mathrm{I}\{X_m = (i_1, \ldots, i_s)\}, \; i_1, \ldots, i_s \in A, - \tag{1}$$

– статистическая оценка для $\mathrm{P}_{i_1,\ldots,i_s}$. Тогда тест обобщенного отношения правдоподобия для проверки $H_0, H_{1(s)}$ имеет вид:

$$\text{принимается} \begin{cases} H_0, \text{ если } \hat{H}_s - s \ln N > -\dfrac{1}{2M} G^{-1}_{N^s - 1}(1-\varepsilon), \\ H_{1(s)} \text{ в противном случае,} \end{cases} \tag{2}$$

где $\hat{H}_s = -\sum_{i_1,\ldots,i_s \in A} \hat{\mathrm{P}}_{i_1,\ldots,i_s} \ln \hat{\mathrm{P}}_{i_1,\ldots,i_s}$ – статистическая оценка s-мерной энтропии Шеннона, $G_K^{-1}(\cdot)$ – обратная функция распределения хи-квадрат с K степенями свободы, $\varepsilon \in (0,1)$ – заданный уровень значимости теста.

Тест (1), (2) удобно использовать для визуализации процесса принятия решений в виде так называемого [9] «энтропийного профиля (портрета)» – графика зависимости нормированного уклонения оценки s-мерной энтропии от ее математического ожидания при H_0:

$$\alpha(s) = b_s\left(\hat{H}_s - E_{H_0}\left\{\hat{H}_s\right\}\right),\ s \in \left\{s_{\min}, s_{\min}+1, \ldots, s_{\max}\right\}. \qquad (3)$$

Для иллюстрации на рис. 1, 2 представлены энтропийные профили генератора, описываемого нелинейной рекуррентой порядка 24 ($N = 2, \varepsilon = 0.05$, $T = 2^{32}/s$) и генератора BelT (СТБ 34.101.27-2011 в режиме гаммирования, $N = 2, \varepsilon = 0.05$, $T = 2^{29}$) соответственно.

Заметим, что для теста (1), (2) опасными оказываются искусственно сформированные «выходные последовательности», являющиеся 2^s-периодическим повторением фрагмента, состоящего из 2^s всевозможных s-цепочек; для таких последовательностей решение всегда будет в пользу H_0. Во избежание этой «бреши» теста необходимо: а) строить энтропийный профиль при различных значениях s; б) оценку $\hat{H}_s$ строить по пересекающимся s-фрагментам.

Отметим еще, что вместо энтропии Шеннона в (1)-(3) могут использоваться энтропийные функционалы Реньи и Тсаллиса [9].

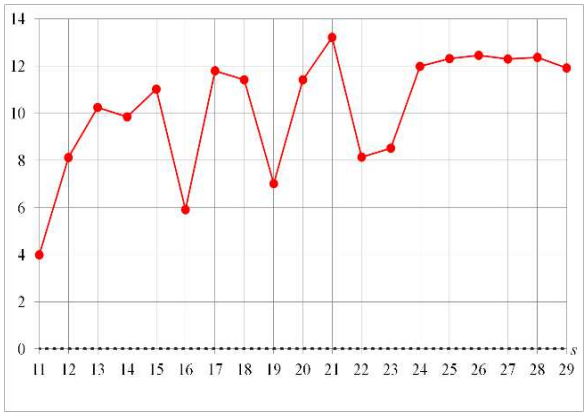

Рис. 1 – Энтропийный профиль $|\alpha(s)|$ нелинейного регистра сдвига в логарифмической шкале

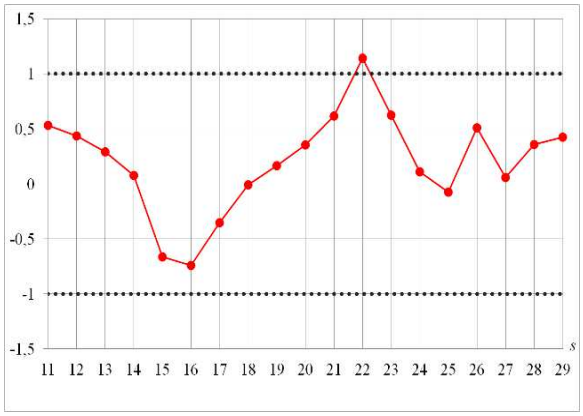

Рис. 2 – Энтропийный профиль $\alpha(s)$ генератора BelT

3. Методы тестирования на основе Марковских моделей s-го порядка

Учитывая, что универсальной (общей) моделью стохастической зависимости элементов выходной последовательности $\{x_t\}$ криптографического генератора является цепь Маркова достаточно высокого порядка s, определим вложенное в H_1

семейство альтернатив марковской зависимости: $H_1^{(s)} = \{\{x_t\}$ – однородная цепь Маркова порядка s с матрицей вероятностей одношаговых переходов P $\}$, где $\mathrm{P} = \left(p_{i_1,\ldots,i_s,i_{s+1}} \right)$, $i_1,\ldots,i_{s+1} \in A$ – $(s+1)$-мерная матрица, $p_{i_1,\ldots,i_{s+1}} = \mathrm{P}\left\{ x_{t+1} = i_{s+1} \mid x_t = i_s,\ldots, x_{t-s+1} = i_1 \right\} \neq N^{-1}$. При $s \to +\infty$ семейство этих альтернатив имеет в пределе альтернативу общего вида $H_1 = \bar{H}_0$.

Тест обобщенного отношения правдоподобия для проверки гипотез H_0, $H_1^{(s)}$ основан на статистической оценке $\hat{h}_s$ условной энтропии $h_s = H\left\{ x_t \mid x_{t-1},\ldots, x_{t-s} \right\}$:

$$\text{принимается} \begin{cases} H_0, \text{ если } \hat{h}_s - \ln N > -G_f^{-1}(1-\varepsilon)/(2(T-s)),\ f = N^s(N-1), \\ H_1^{(s)} \text{ в противном случае.} \end{cases} \quad (4)$$

Аналогично (3) с помощью $\hat{h}_s$ строится энтропийный профиль для $\{x_1,\ldots,x_T\}$.

К сожалению, тесты (3), (4), анализирующие стохастические зависимости глубины s в выходной последовательности $\{x_t\}$, требуют экспоненциально растущей с ростом s длины анализируемой последовательности $T = O\left(N^{s+1}\right)$. Для преодоления этой трудности целесообразно использовать так называемые [3] «малопараметрические модели цепей Маркова высокого порядка», т. е. модели цепей Маркова s-го порядка $\left(N^s \times N\right)$-матрица вероятностей переходов которой зависит от «малого» числа параметров $D \ll N^s(N-1)$.

Приведем известный на сегодня перечень «малопараметрических» моделей, описание которых можно найти в [3]: модель Джекобса – Льюиса; MTD-модель Рафтери; цепь Маркова порядка s с r частичными связями (ЦМ(s,r)); цепь Маркова условного порядка.

Для иллюстрации представим разработанную в БГУ модель ЦМ(s,r) и ее применения для тестирования. Обозначим: $r \in \{1,\ldots,s\}$ – параметр, называемый числом связей; $M_r = (m_1,\ldots,m_r) \in \boldsymbol{M}$ – произвольный целочисленный r-вектор с упорядоченными компонентами $1 = m_1 < m_2 < \cdots < m_r \le s$, называемый шаблоном связей; $Q = \left(q\left(j_1,\ldots, j_{r+1} \right) \right)$, $j_1,\ldots, j_{r+1} \in A$, – некоторая $(r+1)$-мерная стохастическая матрица. Матрица переходов для ЦМ(s,r) имеет следующий малопараметрический вид:

$$p_{i_1,\ldots,i_s,i_{s+1}} = q\left(i_{m_1},\ldots, i_{m_r}, i_{s+1} \right),\ i_1,\ldots,i_{s+1} \in A.$$

Это соотношение означает, что вероятность перехода в будущее состояние зависит не от всех s предыдущих состояний, а лишь от r избранных (согласно шаблону) состояний. Число параметров модели $D_{\text{ЦМ}(s,r)} = N^r(N-1) + r - 1$ может оказаться существен-

но меньше, чем для полносвязной модели ЦМ(s). Например, если $N = 2$, $s = 32$, $r = 3$, то $D_{\text{ЦМ}(s)} = 4.3 \cdot 10^9$, в то время как $D_{\text{ЦМ}(s,r)} = 10$.

В [3] построены статистические оценки для s, r, M_r, Q, а также тест для проверки гипотез H_0, $H_1^{(s)}$ на основе модели ЦМ(s,r). Статистическую оценку $\hat{Q}$ удобно использовать для визуализации уклонения от H_0, когда $q(i_1,\ldots,i_{r+1}) = N^{-1}$. На рис. 3, 4 представлены результаты такой визуализации для генератора со случайной обратной связью и генератора BelT СТБ 34.101.27-2011 в режиме гаммирования.

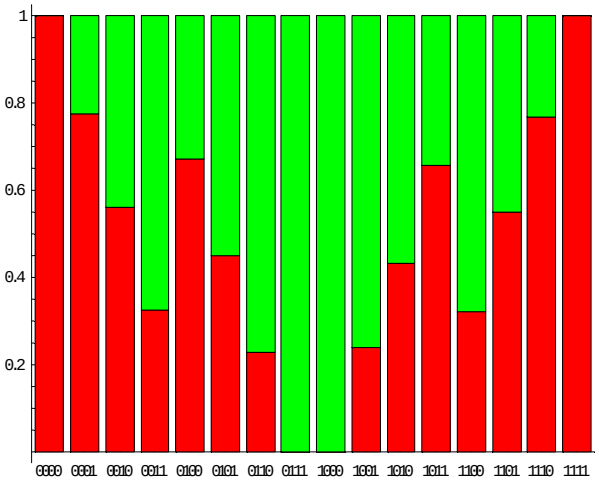

Рис. 3 – Оценка матрицы Q (черный – оценка вероятности перехода в 0, серый – в 1)

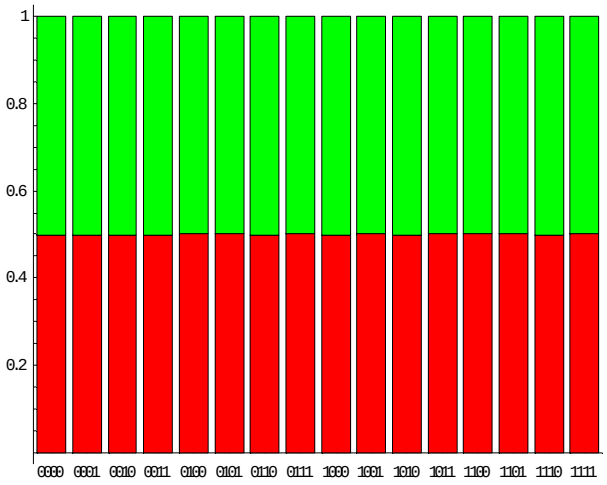

Рис. 4 – Оценка матрицы Q при $s = 32$, $r = 4$, $M_r = (1,4,17,20)$

В [3, 9] приведены алгоритмы тестирования на основе других упомянутых выше малопараметрических моделей.

Список литературы

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001. 380 с.

2. Иванов М.А., Чугунков И.В. Теория применения и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.

3. Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. Криптология. Мн: БГУ, 2013. 512 с.

4. Кнут Д. Искусство программирования. В 3 т. М.: Мир, 1977.

5. Marsaglia G. DIEHARD: a battery of tests of randomness. URL: http://stat.fsu.edu/~geo/diehard.html.

6. Rukhin A. et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST, 2001. URL: http://csrc.nist.gov/rng/SP800-22b.pdf.

7. Information Security Institute. Crypt-X, 1998. URL: www.isi.qut.edu.au.

8. List of General NESSIE Test Tools. URL: www.cryptonessie.org.

9. Харин Ю.С. Статистические оценки энтропии Реньи и Тсаллиса и их использование для проверки гипотез о «чистой случайности» / Ю.С. Харин, В.Ю. Палуха // Весці НАН Беларусі. Серыя фіз.-мат. навук. 2016. № 2. С. 37–47.